UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PATRICE WITFIELD on behalf of herself and all others similarly situated, Plaintiff, v. ATC HEALTHCARE SERVICES, LLC, Defendant.	Case No. 22-CV-5005 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Patrice Whitfield, through her attorneys, bring this Class Action Complaint against Defendant, ATC Healthcare Services, LLC ("ATC" or "Defendant"), alleging as follows:

I. INTRODUCTION

1. ATC, a healthcare staffing company serving healthcare providers across the country, lost control over its employees' highly sensitive personal identifying information ("PII") and personal health information ("PHI") between February and December 2021 in an ongoing data breach by cybercriminals ("Data Breach").

2. On or around December 22, 2021, ATC discovered unusual activity involving employee email accounts. An investigation confirmed that these email accounts were accessed without authorization during most of 2021—between February 9, 2021, and December 21, 2021.

3. On July 1, 2022—more than six months after the Data Breach was discovered and almost eighteen months after the Data Breach first began —ATC issued a Notice of Data Breach Incident (the "Breach Notice") to current and former employees impacted by the Data Breach. The Breach Notice stated that on discovering the Data Breach in late December 2021, ATC

investigated and, on or about May 19, 2022, confirmed that employee email accounts had been accessed and that employee information exposed in the Data Breach contained "names, Social Security numbers, driver's licenses, financial account information, usernames, passwords, passport numbers, biometric data, medical information, health insurance information, electronic/digital signatures and employer-assigned identification numbers." https://atchealthcare.com/notice-of-data-breach-incident/ (last visited August 18, 2022).

4. ATC acknowledges its duty to protect employee confidential information. ATC's Breach Notice stated, the "confidentiality, privacy, and security of information within ATC's care are among ATC's highest priorities." https://atchealthcare.com/notice-of-data-breach-incident (last visited August 18, 2022).

5. Indeed, ATC has a legal duty to protect employee PII and PHI through its policies and state and federal law.

6. On information and belief, ATC failed in that duty because it did not implement or adhere to cybersecurity measures that would have prevented or stopped cybercriminals from accessing its employees' PII and PHI.

7. Following the Data Breach, ATC said that it would "implement[] additional technical safeguards and work[] on additional training and education for our staff on ways to guard against cyber-attacks." https://atchealthcare.com/notice-of-data-breach-incident/ (last visited August 18, 2022). These are security measures ATC should have implemented *before* the Data Breach.

8. ATC's negligent conduct puts Plaintiff and ATC's current and former employees at risk.

9. Armed with employees' PII and PHI, data thieves can commit various crimes

including, e.g., opening new financial accounts in employees' names, taking out loans in employees' names, using employees' names to obtain medical services, using employees' information to obtain government benefits, filing fraudulent tax returns using employees' information, obtaining driver's licenses in employees' names but with another person's photograph, and giving false information to police during an arrest.

10. As a result of the Data Breach, ATC's current and former employees have been exposed to a heightened and imminent risk of fraud and identity theft. They must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Employees also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII and PHI was accessed during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to ATC's data security systems, future annual audits, and adequate credit monitoring services funded by ATC.

II. PARTIES

14. Plaintiff, Patrice Whitfield, is a natural person and citizen of Illinois, residing in Riverdale, Illinois, where she intends to remain. Plaintiff is a former ATC employee, where she was employed from October 2015 through August 2019 as a Certified Nursing Assistant. Plaintiff is a Data Breach victim, having received ATC's Breach Notice in July 2022.

15. Defendant ATC Healthcare Services LLC is a Georgia limited liability company, with its principal place of business at 1983 Marcus Avenue, Suite E-122, Lake Success, New

York 11042-1029.

III. JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because ATC maintains its principal place of business this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

IV. BACKGROUND FACTS

A. ATC

19. ATC is healthcare staffing company and a healthcare franchise. ATC's mission is to become "the go-to resource nationwide for healthcare communities in need of qualified staff.[1] ATC's website encourages healthcare professional to join the ATC team for its flexible work schedules and outstanding benefits.[2]

20. Upon information and belief, ATC has approximately 4,000 employees across the country.

21. ATC's privacy policy promises to protect the sensitive information it collects by using "vulnerability scanning and/or scanning to PCI standards." ATC says it never asks for

[1] https://atchealthcare.com/about/our-story/ (last visited August 18, 2022)
[2] *Id.*

credit card numbers and uses "Malware Screening."[3]

22. ATC further promises, "We do not sell, trade or otherwise transfer to outside parties your Personally Identifiable Information."[4]

23. But, on information and belief, ATC fails to strictly adhere to its own policies in maintaining its employees' PII and PHI.

B. ATC Fails to Safeguard Employee PII and PHI

24. Plaintiff is a former employee of ATC.

25. As a condition of employment with ATC, employees were required to disclose their PII and PHI.

26. ATC collects and maintains employee PII and PHI in its computer systems even after employees no longer work for ATC.

27. In collecting and maintaining the PII and PHI of current and former employees, ATC agreed it would safeguard the data according to its internal policies and state and federal law.

28. Even so, on or about February 9, 2021, hackers bypassed ATC's security systems and accessed employee PII and PHI.

29. Hackers did so undetected, as ATC would not discover the hack until more than nine (9) months later, on or about December 22, 2021.

30. By the time ATC discovered the Data Breach, cybercriminals had already accessed its employees' PII and PHI, including names, Social Security numbers, driver's licenses, financial account information, usernames, passwords, passport numbers, biometric data, medical information, health insurance information, electronic/digital signatures, and employer-

[3] https://atchealthcare.com/privacy-policy/ (last accessed August 18, 2022).
[4] *Id.*

assigned identification numbers.

31. After discovering the Data Breach, ATC claims it initiated an investigation to determine the nature and scope of the event. ATC says the investigation confirmed that the email accounts were accessed without authorization at varying times between February 9, 2021, and December 22, 2021. A true and correct copy of the Breach Notice is attached as **Exhibit A**.

32. ATC says, "in an abundance of caution," it then undertook to identify what information was present in the impacted email accounts. ATC completed the first phase of this investigation on May 19, 2022.

33. Thereafter, ATC worked "to reconcile the information with our internal records in furtherance of identifying the individuals to whom the data related and the appropriate contact information for the relevant individuals." *Id.* ATC says by June 2, 2022, it completed this investigative phase. However, inexplicably it took ATC yet another month to publicly disclose the Data Breach and to notify Data Breach victims. *Id.*

34. On information and belief, cybercriminals could breach ATC's systems because ATC failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII and PHI. ATC's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII and PHI. Further, the Breach Notice makes clear that ATC has since implemented "additional training and education for our staff on ways to guard against cyber-attacks." *Id.*

C. Plaintiff's Experience

35. Plaintiff Whitfield is a former ATC employee.

36. As a condition of Plaintiff's employment, ATC required her to provide her PII and PHI.

37. Plaintiff provided her PII and PHI to ATC and trusted that the company would

use reasonable measures to protect it according to ATC's internal policies and state and federal law.

38. As a result of the Breach Notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Breach Notice, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

39. Since the Data Breach occurred, Plaintiff's debit card has been compromised three (3) times. Just three months ago, Plaintiff's bank account was compromised, and she was forced to close the account and open a new one.

40. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII and PHI was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

41. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

42. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

43. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and

safeguarded from future breaches.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

44. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

45. As a result of ATC's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in its possession.

46. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and

PHI can be worth up to $1,000.00 depending on the type of information obtained.

47. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

48. It can take victims years to spot identity or PII/PHI theft, giving criminals plenty of time to use that information for cash.

49. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

50. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

51. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

52. Defendant disclosed the PII and PHI of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII and PHI of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

53. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant failed to adhere to FTC guidelines.

54. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII and PHI.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

56. The guidelines also recommend that businesses watch for large amounts of data

being transmitted from the system and have a response plan ready in the event of a breach.

57. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Ignored Best Practices for Healthcare Providers

61. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

62. Several best practices have been identified that, at a minimum, should be implemented by healthcare providers like Defendant, including but not limited to: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

G. Defendant's Conduct Violates HIPAA Standards of Care and Evidences Its Insufficient Data Security

66. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive health information.

67. Covered entities and their business agents (including Defendant) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

68. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

69. A Data Breach such as the one Defendant experienced is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

70. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[5]

71. Defendant's Data Breach resulted from a combination of insufficiencies that

[5] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4 (last visited August 18, 2022).

demonstrate ATC failed to comply with safeguards and standards of care mandated by HIPAA regulations, resulting in the unauthorized access to the PII and PHI of Defendant's current and former employees.

V. CLASS ACTION ALLEGATIONS

72. Plaintiff sues on her own behalf and on behalf of the proposed classes ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class**: All individuals residing in the United States whose PII and/or PHI was compromised in the Data Breach.
>
> **Illinois Subclass:** All individuals residing in Illinois whose PII and/or PHI was compromised in the Data Breach.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

73. Plaintiff reserves the right to amend the class definition.

74. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff represents the proposed Class, consisting of at least 4,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interest does not conflict with the Class's interests and Plaintiff has

retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII and PHI;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII and PHI;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. Whether Defendant violated 740 ILCS 14/15(d);

ix. What the proper damages measure is; and

x. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

75. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

VI. COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

76. Plaintiff realleges all previous paragraphs as if fully set forth below.

77. Plaintiff and members of the Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

78. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII and PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

79. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Defendant also

owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

80. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII and PHI.

81. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII and PHI.

82. PII and PHI are highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff's and members of the Class's and the importance of exercising reasonable care in handling it.

83. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and

exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

84. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

VII. COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

85. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

86. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII and PHI.

87. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII and PHI. The FTC publications and orders promulgated pursuant to the

FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII and PHI.

88. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and PHI and by not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

89. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

90. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard PII and PHI.

91. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII and PHI.

92. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

93. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class would not have been injured.

94. The injury and harm suffered by Plaintiff and members of the Class was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should

have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

95. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII and PHI, Plaintiff and members of the Class would not have entrusted Defendant with their PII or PHI.

96. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

VIII. COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

97. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

98. Defendant offered to employ Plaintiff and members of the Class in exchange for their PII and PHI.

99. In turn, and through internal policies, Defendant agreed it would not disclose the PII or PHI it collects to unauthorized persons. Defendant also promised to safeguard employee PII and PHI.

100. Plaintiff and the members of the Class accepted Defendant's offer by providing PII and PHI to Defendant in exchange for employment with Defendant.

101. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII and PHI

102. Plaintiff and members of the Class would not have entrusted their PII or PHI to Defendant in the absence of such agreement.

103. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII and PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted.

104. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

105. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

106. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act

with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

107. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

108. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

109. In these and other ways, Defendant violated its duty of good faith and fair dealing.

110. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

IX. COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

111. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

112. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

113. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment.

114. Defendant appreciated or had knowledge of the benefits conferred upon itself by

Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII or PHI, as this was used to facilitate their employment.

115. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their PII or PHI because Defendant failed to adequately protect their PII and PHI. Plaintiff and the proposed Class would not have provided PII or PHI or worked for Defendant at the payrates they did, had they known Defendant would not adequately protect their PII or PHI.

116. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

X. COUNT V
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Nationwide Class)

117. Plaintiff incorporates all previous paragraphs as if fully set forth below.

118. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

119. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and members of the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen

data.

120. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII and PHI with which it is entrusted, specifically including information pertaining to financial records it obtains from its employees, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

121. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its employees' (i.e., Plaintiff's and members of the Class's) data.

122. If an injunction is not issued, Plaintiff and members of the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and members of the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and members of the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and members of the Class, which include monetary damages that are not legally quantifiable or

provable.

123. The hardship to Plaintiff and members of the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

124. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, members of the Class, and the public at large.

XI. COUNT VI

Violation of 740 ILCS 14/15(d)
(On Behalf of Plaintiff and the Illinois Subclass)

125. Plaintiff incorporates all previous paragraphs as if fully set forth below.

126. Defendant collects, and is thus in possession of, biometric identifiers or biometric information, as defined in 740 ILCS 14/10, of Plaintiff and its current and former employees.

127. Defendant's Breach Notice admits that biometric identifiers and/or information was compromised in the Data Breach. This resulted in the disclosure of Plaintiff and the Illinois Subclass's biometric identifiers and/or information without Plaintiff's and the Illinois Subclass's consent in violation of the Illinois Biometric Privacy Act, 740 ILCS 14/15(d).

128. Defendant's unlawful conduct is negligent and reckless because BIPA has governed the collection and use of biometric identifiers and biometric information since 2008, and Defendant is presumed to know these legal requirements.

129. Defendant's unlawful conduct caused injury to Plaintiff and the Illinois Subclass.

130. Plaintiff and the Illinois Subclass seek damages, including statutory damages, attorney' fees, and costs.

XII. PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII/PHI;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

XIII. JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 23rd day of August, 2022.

/s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
T: (212) 558-5500
F: (212) 344-5461
jbilsborrow@weitzlux.com

Samuel J. Strauss (*pro hac vice* forthcoming)
Raina C. Borrelli (*pro hac vice* forthcoming)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
T: (608) 237-1775
F: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff